(12) UK Patent Application (19) GB (11) 2 317 308 (13) A

(43) Date of A Publication 18.03.1998

(21) Application No 9718373.5

(22) Date of Filing 29.08.1997

(30) Priority Data
(31) 08227970 (32) 29.08.1996 (33) JP

(71) Applicant(s)
Kokusai Denshin Denwa Co Ltd

(Incorporated in Japan)

3-2 Nishishinjuku 2-chome, Shinjuku-ku, Tokyo 163, Japan

(72) Inventor(s)
Osamu Maeshima
Yoshihiro Ito
Masami Ishikura

(74) Agent and/or Address for Service
Boult Wade Tennant
27 Furnival Street, LONDON, EC4A 1PQ, United Kingdom

(51) INT CL[6]
H04L 12/46 12/56

(52) UK CL (Edition P)
H4P PPA

(56) Documents Cited
EP 0790751 A2
Data Communications International, Vol.25, No.7, 21 May 96, USA, pp85-90 IEICE Trans. on Communications, Vol.E78-B, No.8, Aug 95, Japan, pp1208-18 ConneXions, Vol.8, No.8, Aug 94,USA, pp8-17

(58) Field of Search
UK CL (Edition P) H4P PPA PPS
INT CL[6] H04L 12/46 12/56 12/66
Online: WPI, INSPEC

(54) Method for constructing a VPN having an assured bandwidth

(57) An IP tunnel 101 is constructed between routers 300A and 300B connected with the INTERNET 100. A bandwidth of the IP tunnel 101 is assured by setting-up a reservation resource protokol (RSVP) on the IP tunnel 101. Further as a traffic control of the routers 300A, 300 and 300B on the IP tunnel 101, a frequency for sending packets, which are processed by an input processor and an output processor inside of the router, is allotted based on a ratio of the reserved bandwidth in each IP tunnel, the an algorithm for controlling the traffic is simplified. Furthermore each of the routers 300A, 300 and 300B on IP tunnel 101 has a function for scheduling a reservation and manages a time period at which a Virtual Private Network (VPN) of a type of the reservation resource protokol (RSVP) will be used, then it is possible to reserve the assurance of the bandwidth on a designated date and time in future.

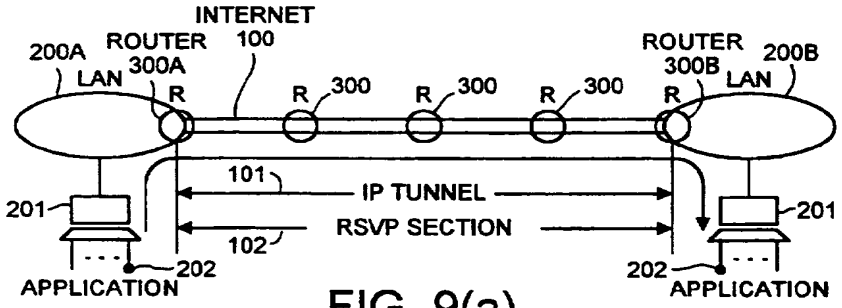

FIG. 9(a)
EMBODIMENT OF THE INVENTION

GB 2 317 308 A

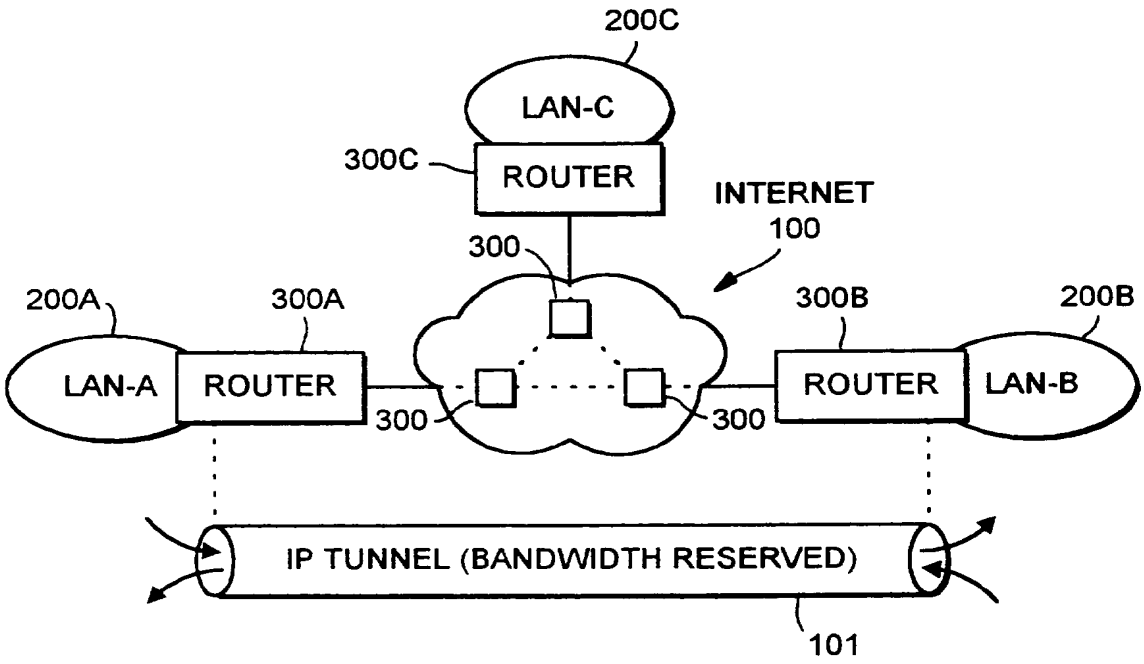

FIG. 1
NETWORK MODEL

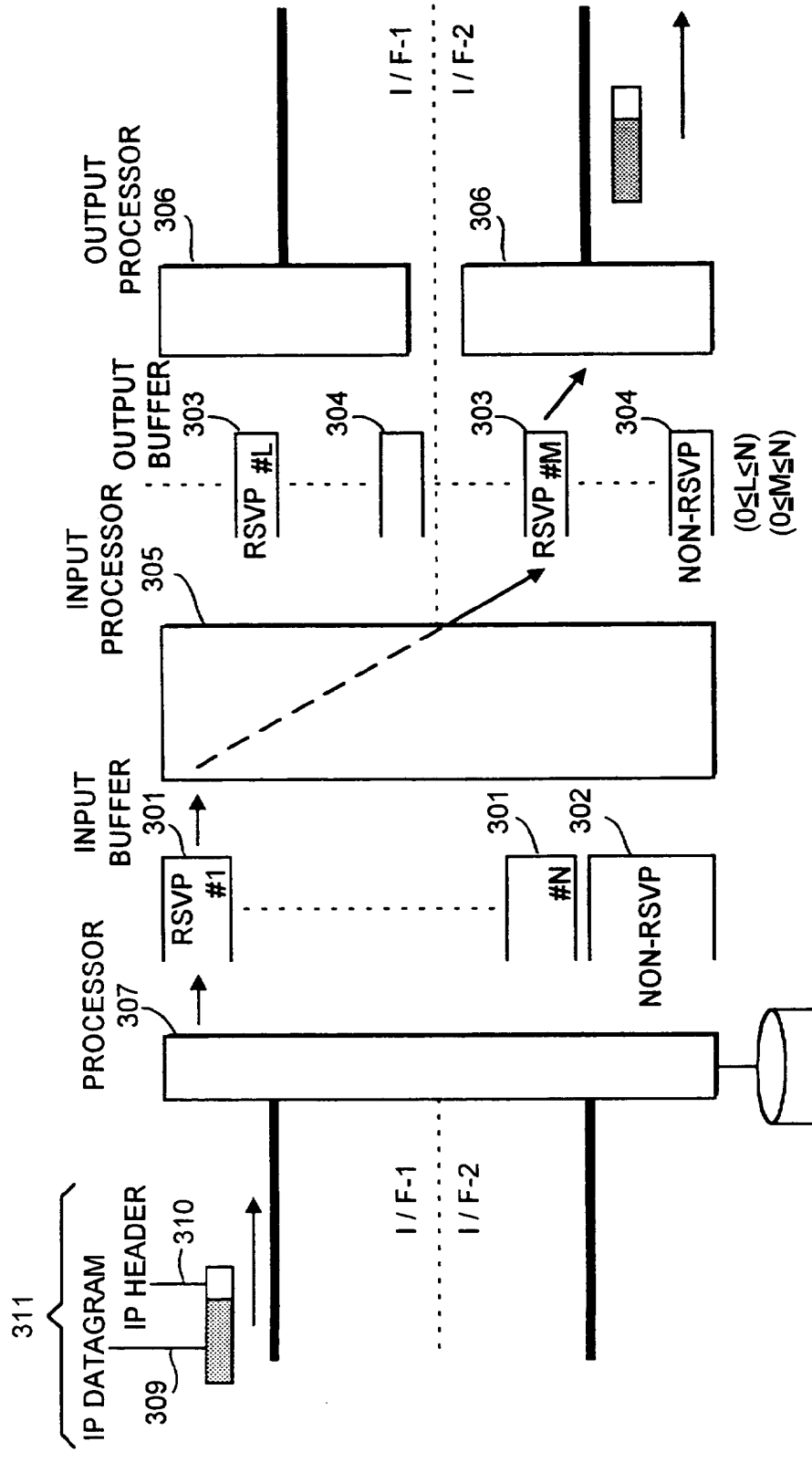

FIG. 2
TRAFFIC CONTROL IN ROUTER

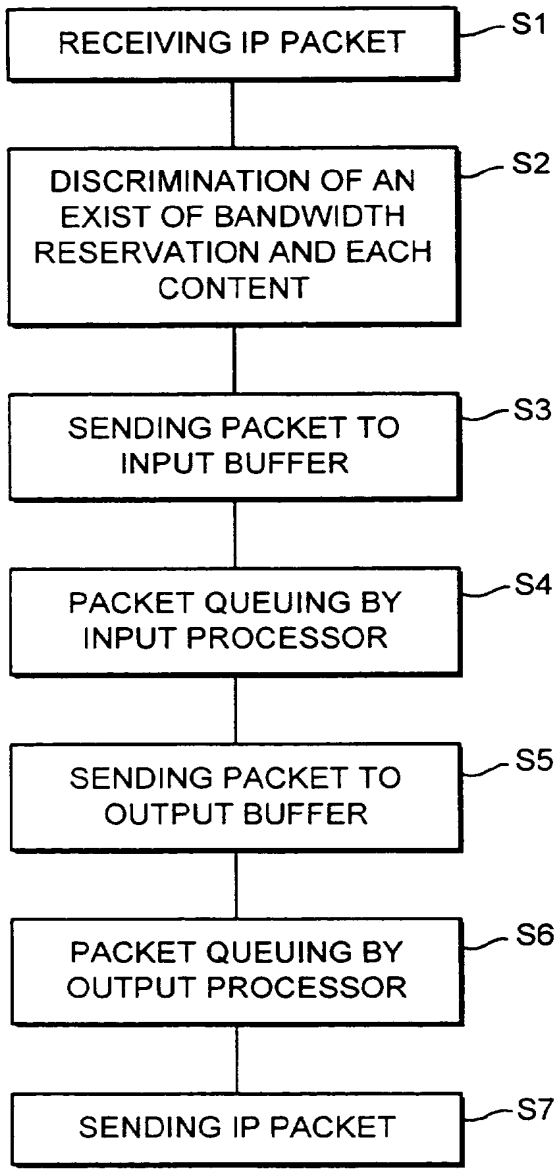

FIG. 3

TRAFFIC CONTROL IN ROUTER

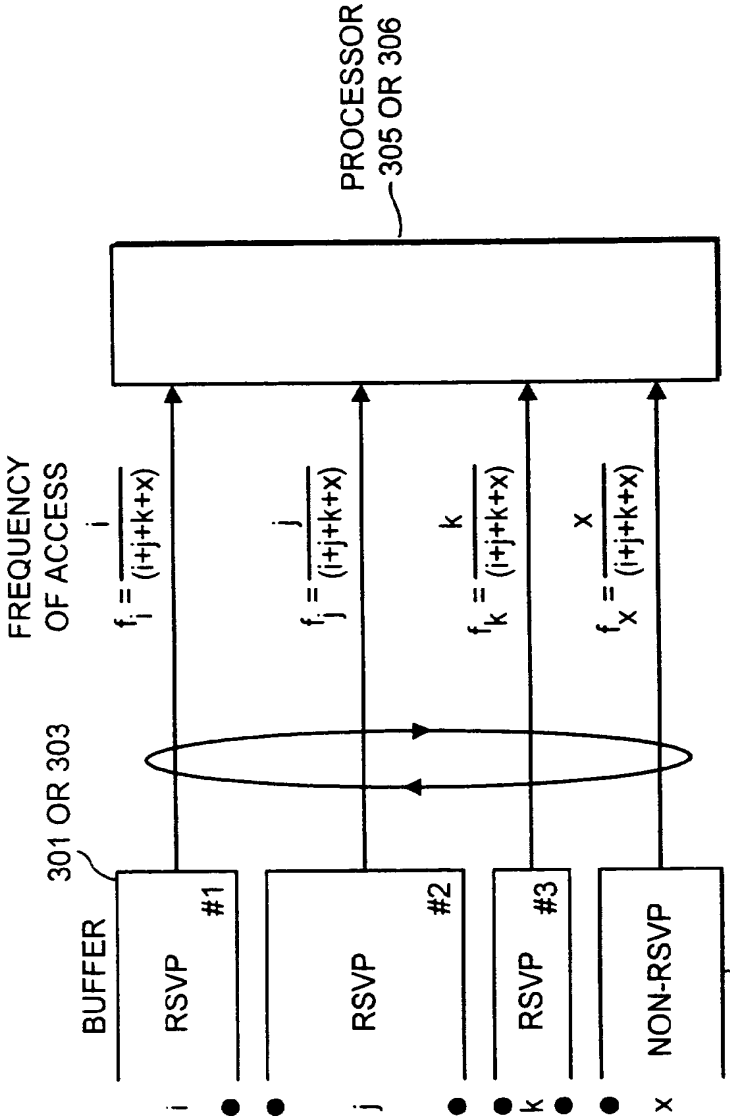

FIG. 4
PACKET QUEUING

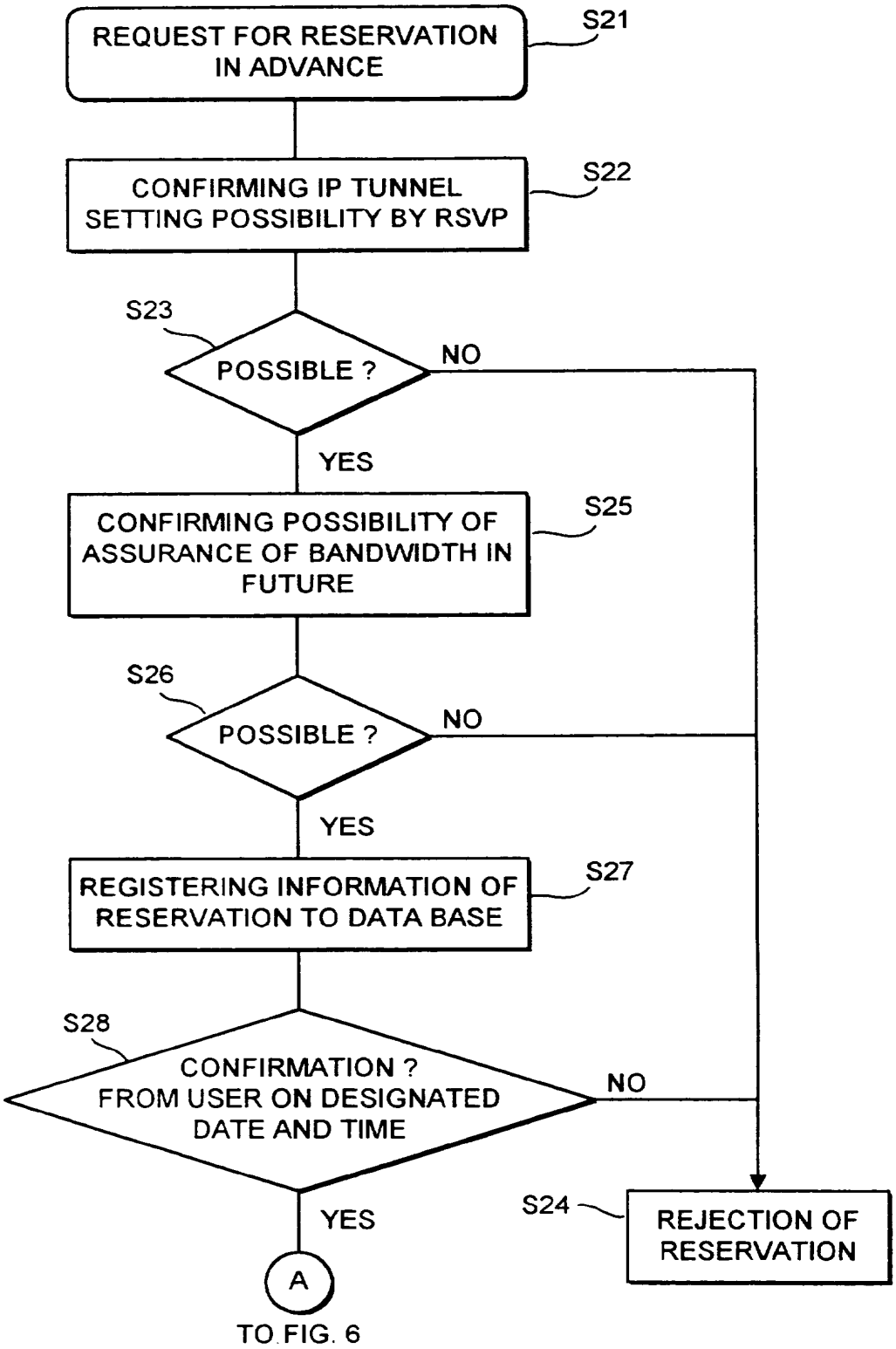

FIG. 5

RESERVATION SCHEDULING IN VPN

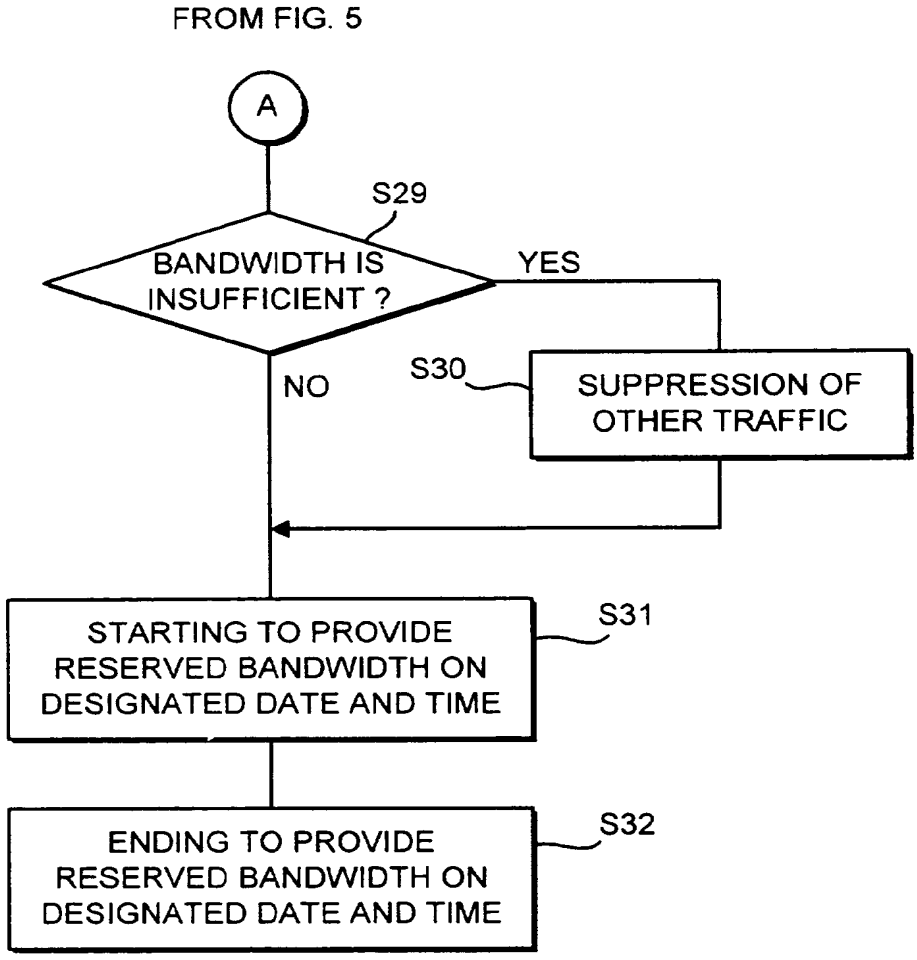
FROM FIG. 5
A
S29
BANDWIDTH IS INSUFFICIENT ?
YES
NO
S30
SUPPRESSION OF OTHER TRAFFIC
STARTING TO PROVIDE RESERVED BANDWIDTH ON DESIGNATED DATE AND TIME
S31
ENDING TO PROVIDE RESERVED BANDWIDTH ON DESIGNATED DATE AND TIME
S32

FIG. 6

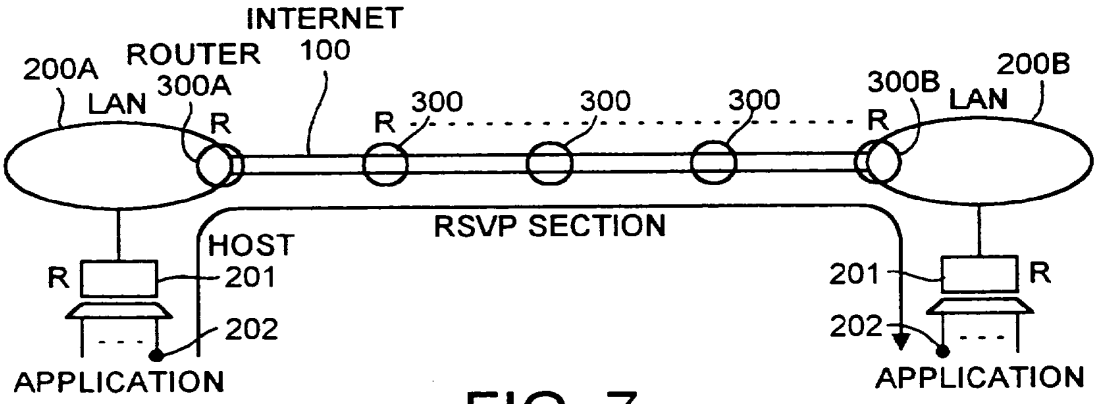

FIG. 7
PRIOR ART (RSVP)

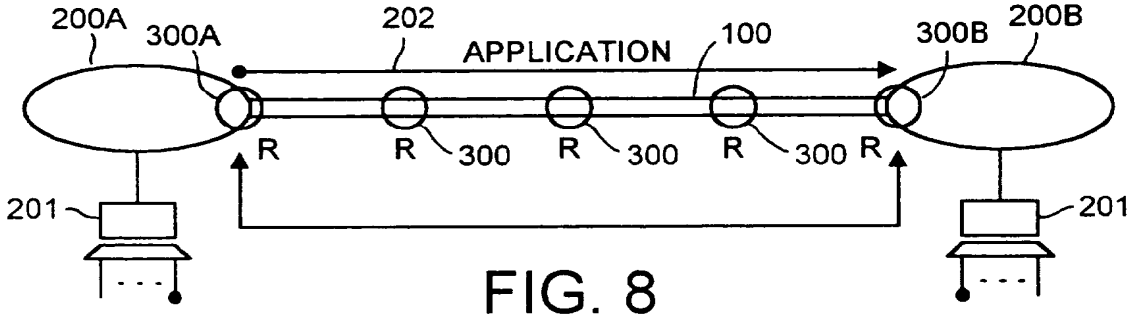

FIG. 8
PRIOR ART

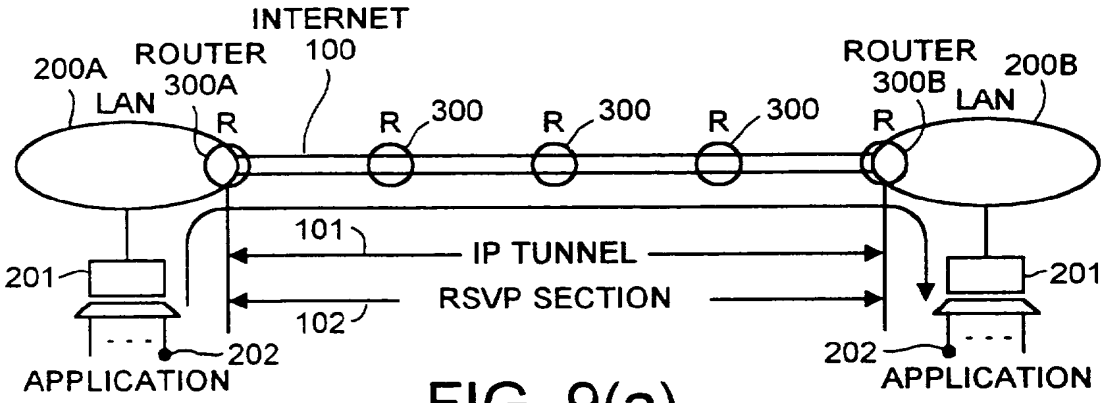

FIG. 9(a)

EMBODIMENT OF THE INVENTION

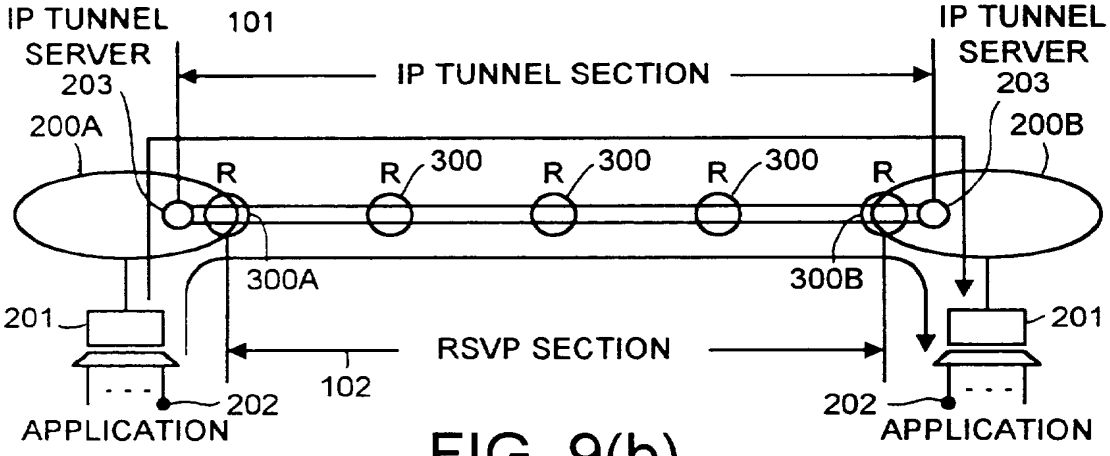

FIG. 9(b)

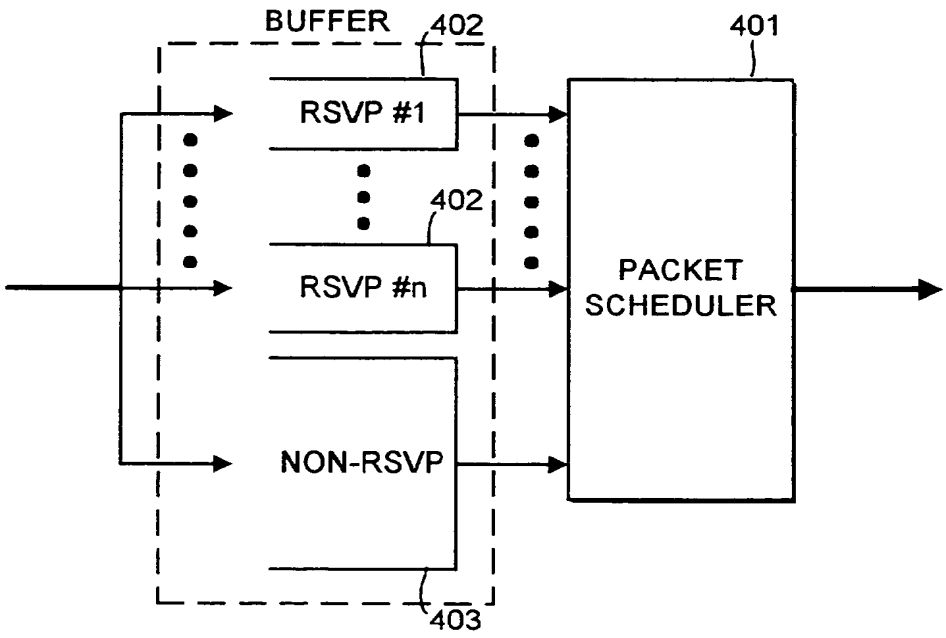

FIG. 10

EMBODIMENT OF THE INVENTION
(PACKET SCHEDULING)

Specification

TITLE OF THE INVENTION

Method for constructing a VPN having an assured bandwidth

FIELD OF THE INVENTION

This invention relates to a method for constructing a VPN(Virtual Private Network) on the INTERNET, especially relates to assurance and/or reservation of a bandwidth by every host and/or sub-network.

BACKGROUND OF THE INVENTION

The VPN is a network which constructs logical groups on a public network such as the INTERNET, wherein the logical groups are mutually closed.

Generally, the public network such as the INTERNET is connected by the non-specific masses. Therefore, there is a security problem that it is not possible to avoid a dishonest access by a third party, because principally it is not possible that only specific users telecommunicate each other.

Therefore, recently the VPN technique is watched. According to the VPN technique, a dedicated line is virtually constructed on the INTERNET by considering a counterplan of the security of end to end, and, the dedicated line is used as a mainstay between LAN and LAN (Local Area Network).

Concretely, in the prior art of the VPN, a security is carried out by an encryption of data between end and end, an authentication of a user and a control of an access, then a closed group is provided by connecting specific points via the INTERNET.

By constructing VPN on the public network, it is possible for only

specific users to communicates each other, and it is possible to use the INTERNET as a dedicated line.

However, because of its specification, the prior VPN does not assure network resources such as a bandwidth.

Namely, the prior VPN is different from an original dedicated line in that the bandwidth is variable by an influence of other traffics and that it is difficult to predict its telecommunication characteristics.

On the other hand, an RSVP is known. Wherein, the RSVP is a resource reservation protokol which attaches importance to a QoS (Quality of Service; bandwidth, delay, flicker).

Concretely, as shown in Fig.7, all host terminals 201 in the specific LAN 200A and 200B connected with the INTERNET 100 and all reuters 300A, 300B and 300C between LAN 200A and 200B must support the RSVP in each application as a unit. In Fig.7, a mark R indicates a support of RSVP.

Therefore, by the RSVP in each application, the user requests a network resource which satisfies a specific service quality for example a specific bandwidth to the network, then the user assures it.

Namely, in the prior art, the network resource has been reserved between end and end in each application as a unit by the RSVP.

By the way, as shown in Fig.1, if the routers 300A, 300B and 300C only support the RSVP in each application, an application on the RSVP can not be connected with both LAN 200A and 200B, because the application is terminated by the routers 300A and 300B at both ends.

In a case of intending to assure the bandwidth of the VPN by combining prior art VPN with the RSVP, there are following problems (1) and (2).

(1) Since the network resources are assured by RSVP between end and end, all hosts connected to VPN must support RSVP.

(2) In the present utilization of VPN, a management in each host or sub-network as a unit is recommended than each application. In such case, an assurance of the bandwidth in each application is not proper. Wherei n, the sub-network is a network which is made by further dividing a host part of the IP address into a network part and host part. For example, the LAN 200A or LAN 200B in Figs.7 and 8 is divided into sub-networks.

It is therefore desirable to provide a method for constructing a VPN which assures a bandwidth in each host or in each sub-network as a unit.

SUMMARY OF THE INVENTION

According to the present invention, there is provided a method for constructing a VPN having assured bandwidth which comprises steps of:

a step of constructing an IP tunnel between routers connected with the INTERNET;

a step of reserving a bandwidth of said IP tunnel by setting-up a reservation resource protokol (RSVP) on said IP tunnel.

In an embodiment of the present invention, further as a traffic control of said router on said IP tunnel, a frequency for sending packets, which are processed by an input processor and an output processor inside of said router, is allotted based on a ratio of the reserved bandwidth in each IP tunnel.

In another embodiment, further each of said routers on said IP tunnel has a function for scheduling a reservation and manages, based on the reservation schedule, a time period at which said reservation resource protokol is used.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a network model to which the present invention is applied.

Fig. 2 shows a configuration of a traffic control in a router.

Fig. 3 shows a process of the traffic control in the configuration shown in Fig.2.

Fig. 4 shows a packet queuing in the traffic control.

Fig. 5 shows a process of a reservation schedule of VPN in the router.

Fig. 6 shows a process of a reservation schedule of VPN in the router.

Fig. 7 shows a conventional RSVP.

Fig. 8 shows a fault of the conventional RSVP when a host of a LAN does not support RSVP.

Fig. 9(a) shows an embodiment of the present invention.

Fig. 9(b) shows an embodiment of the present invention.

Fig. 10 shows an explanation for simplifying an algorism of a packet scheduling.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

An embodiment of the present invention will be explained referring to Figs.9(a), 9(b) and 10.

In an example shown in Fig.9(a), an IP (Internet Protokol) tunnel 101 is constructed between a router 300A and a router 300B respectively connected with the INTERNET. As well-known, the IP tunnel is a section where a packet exists, wherein said packet is constructed by adding or encapsulating, to an original packet, an IP header which has an IP address of the router 300A and an IP address of the router 300B (a start point and an end point of the IP tunnel 101) etc. An router in the end

point, for example the router 300B, removes the IP header.

Therefore, the IP tunnel 101 becomes a VPN for the LAN 200A and the LAN 200B by passing, through the IP tunnel 101, all traffics between the LAN 200A and the LAN 200B which are belonged to the routers 300A and 300B at both ends.

Each of the routers 300A, 300B and 300C on the IP tunnel 101 supports a RSVP (Reservation Resource Protokol), then these routers set up the RSVP on the IP tunnel 101. Each application 202 on both LAN 200A and 200B is encapsulated at the start point of the IP tunnel, because a bandwidth is assured at the IP tunnel 101 (between routers 300A and 300B) by the RSVP. Then, it is possible for the application 202, as the data adaptive to the RSVP between routers 300A and 300B, to use network resource (for example, a bandwidth) assured on the IP tunnel.

Wherein, as shown in fig.9(b), a section of the IP tunnel 101 at least includes a section where the RSVP assures the bandwidth (for example, a section between routers 300A and 300B).

Namely, it is possible to reserve a bandwidth in every IP tunnel. The bandwidth is reserved not by each application but by each host or each sub-network in the LAN 200A and 200B. It is not necessary for the host 201 to support the RSVP.

The reservation of the bandwidth is cancelled by sending a message of cancellation by the RSVP from the router 300A (or 300B) to others 300 and 300B (or 300 and 300A).

Since the bandwidth in assured on the RSVP, it is not necessary to change a parameter of each node by manual, then a human cost can be deleted. Further, it is possible to speedily and flexibly allocate the bandwidth according to a short-term demand. Furthermore, it is easy to cancel the assured bandwidth.

As mentioned-above, by combining the IP tunnel 101 with the RSVP, it is possible to construct the VPN which enables to assure the bandwidth in host 201 or sub-network as a unit without receiving the influence of another traffic.

By the way, while the RSVP is a protokol for reserving and establishing a network resource, it dose not prescribe a concrete method for controlling a QoS (bandwidth, delay, flicker etc.). Therefore, a assurance of the QoS in the network is depend on a traffic control of the router and/or a switch. A WFQ (Weight Fair Queuing) is a complex algorism, because it controls a bandwidth and a delay by determining a priority according to a traffic characteristics of an application, wherein the WFQ is known as an algorism for a packet and/or a scheduling.

In this case, since only bandwidth as the network resource is reserved, it is possible to control the assurance of the bandwidth by a simple algorism of a packet scheduling as shown in Fig.10 except for said complex algorism of WFQ. Especially, the traffic control of each router 300A, 300 or 300B on the IP tunnel 101 is simplified by using an algorism that a frequency or a number of packets which are processed by an input processor and an output processor inside of said routers 300A, 300 and 300B, is allotted based on a ratio of the bandwidth reserved in each IP tunnel 101.

In fig.10, the packet schedule is carried out by a packet scheduler 401, a buffer 402 for plural RSVP (IP tunnel) #1～#n and a buffer 403 for non RSVP (a protokol except for RSVP). Namely, since a bandwidth between adjacent routers is divided to a bandwidth for each of the plural IP tunnels and a bandwidth for others (a bandwidth for non IP tunnel), a buffer space in the each router is divided to the buffer 402 for the plural IP tunnels and the buffer 403 for others (for non IP

tunnel). It is assumed that a packet is arrived at each buffer 402 for RSVP with same distribution of a traffic characteristics. Then, an algorism is simplified by allotting a buffer size of each buffer 402 for RSVP and a frequency for packets which are send from each buffer 402 for RSVP by the scheduler 401 based on a ratio of the reserved bandwidth in each IP tunnel. Wherein, the buffer 403 for non RSVP sends out a packet in a low priority. For example, the buffer 403 for non RSVP sends out a packet when no packet is in the buffer 402 for RSVP.

Furthermore, in the reservation of the network resources by using the original RSVP, the network resources are reserved only when the resources are necessary. However, in the present invention, it is possible to extend the original RSVP and to designate a date or a time when the reserved bandwidth will be used, because each of routers 300A, 300 and 300B on the IP tunnel 101 has a function for scheduling a reservation and manages a time period at which VPN of a type of a reservation resource is used.

An embodiment of the present invention will be explained referring to Figs.1~6.

In a network model shown in Fig.1, three LANs 200A, 200B and 200C are connected with the INTERNET via routers 300A, 300B and 300C which support RSVP. A router 300 on the INTERNET also supports RSVP. An IP tunnel 101 is set between the router 300A and the router 300B, also an IP tunnel is set between the router 300B and the router 300C, and, an IP tunnel is set between the router 300C and the router 300A. Then, all traffics between LAN 200A and LAN 200B are passed through the IP tunnel 101, all traffics between LAN 200B and LAN 200C are passed through the IP tunnel between the router 300B and the router 300C, and, all traffics between LAN 200C and LAN 200A are passed through the IP tunnel

between the router 300C and the router 300A.

The IP tunnel 101 is set by adding an Ip tunnel function only on a machine (IP tunnel server) at both ends of the IP tunnel 101. Namely, a router at one end of the IP tunnel (for example, the router 300A) request the setting of the IP tunnel to a router at another end of the IP tunnel (for example, the router 300B), then the IP tunnel is set.

As mentioned-above, encapsulation or cancellation of the IP packet at a start point or an end point of the IP tunnel is carried out in a range including a section 102 (shown in fig.9) where a bandwidth is assured by RSVP. Therefore, it is possible that the Ip tunnel function is added by a provider of a bandwidth (for example, telecommunication carrier). Further, as shown in Fig.9(b), it is possible for a user of the bandwidth to add the Ip tunnel function on LANs 200A and 200B by using a IP tunnel server 203.

Furthermore, in this embodiment, a security is carried out by an encryption of data between LAN 200A and 200B, between LAN 200B and 200C, and, between LAN 200C and 200A, an authentication of a user and a control of an access, then LANs 200A, 200B and 200C are connected each other via the INTERNET.

The router is constructed as shown in Fig.1 for controlling the traffics. In this embodiment, each router has two input interfaces and two output interfaces, because usual router has plural input interfaces and plural output interfaces.

In the router, at a process for assuring a bandwidth by RSVP before data transmission, the input buffer 301 for RSVP and one input buffer 302 for non RSVP (for non-reserved-type packet) are set in a input side, and the output buffer 303 for RSVP and the output buffer 304 for non RSVP are set in output side. A number N of the input buffer 301 is the same number of the IP tunnel (a number of reservation). A

number L+M of the output buffer 303 is larger than the number of the IP tunnel (a number of reservation). One output buffer 304 is set in each output interfac e. Wherein, a size of each buffer is variable according to the bandwidth reserved to each IP tunnel.

Further, the router comprises an input processor 305, an output processor 306 for each output interfaces, an processor 307 for identifying a reservation and a reservation data-base 308 linked to the processor 307. In the data base 308, an existence of a bandwidth reservation and data which is necessary to identify, verify and confirm each content of a reservation (for example, IP address of sending side, IP address of receiving side, port number, protokol ID, reserved bandwidth, etc.) are stored. In fig.2, 309 denotes an original packet (IP datagram), 310 denotes an IP header in which the IP address of the routers at both ends of the IP tunnel and 311 denotes a encapsulated packet to which the IP header 310 was added.

The reservation of the bandwidth to the IP tunnel is carried principally when a host or a sub-network on LAN needs the bandwidth. For the reservation, the host or sub-network informs a request for an assurance of a bandwidth to a router at one end of a section where a bandwidth is assured by RSVP, and, informs a content (for example, IP address of sending side, IP address of receiving side, port number, protokol ID, reserved bandwidth, etc.) of a reservation. The router transfers these information to other routers on a way and a router at another end of the IP tunnel by RSVP. Each router stores the reservation of the bandwidth and its content in the data-base 308. If a certain router can not reserve the bandwidth, the router informs a message indicating a rejection of the request to the router at the point.

A traffic control in the router will be explained referring to Figs.2 ~4.

(1) As steps S1 ~ S2 shown in Fig.3, referring to the data-base 308, the processor 307 identifies, verifies and confirms an existence of a bandwidth reservation and each content of a reservation (for example, IP address of sending side, IP address of receiving side, port number, protokol ID, reserved bandwidth, etc.) to packets arrived at each input interface.

(2) After identification, verification and confirmation of the existence of a bandwidth reservation and the content of each reservation, as steps S3 shown in Fig.3, the processor 307 allocates the packets to the input buffer corresponding to the reserved IP tunnel.

(3) At a transferring the packets, the input processor 305 obtains a packet from the input buffer having a high priority, as follows①~②.

① As show in Fig.4, it is assumed that three buffers #1,#2,#3 are used as the input buffer 301 for RSVP, one input buffer 302 for non-RSVP is used and a ratio of each reserved bandwidth of IP tunnel and non reserved bandwidth is i:j:k:x.

② The input processor 305 takes out the packet from each input buffer by accessing each input buffer with a frequency fm according to the ratio of the bandwidth. Concretely, the frequency fm is indicated by fm=m/(i+j+k+x), wherein m is any one of i,j,k and x. If no packet exists in all input buffers #1~#3 for RSVP when the input processor 305 accesses to these buffers, the input processor 305 accesses to the input buffer 302 for non-RSVP. If a packet exists in the input buffer 302, the input processor 305 takes it out form the buffer 302.

(4) After processing to the input buffers, the input processor transfers the packet to corresponding output buffer.

(5) As steps S6 ~S7 in Fig.3, the output processor 306 corresponding to

each output interface takes out the packet from the output buffer. Namely,

① As show in Fig.4, it is assumed that three buffers #1,#2,#3 are used as the output buffer 303 for RSVP, one output buffer 304 for non-RSVP is used and a ratio of each reserved bandwidth of IP tunnel and non reserved bandwidth is i:j:k:x.

② The output processor 306 takes out the packet from each output buffer by accessing each output buffer with a frequency fm according to the ratio of the bandwidth. Concretely, the frequency fm is indicated by fm=m/(i+j+k+x), wherein m is any one of i,j,k and x. If no packet exists in all output buffers #1～#3 for RSVP when the output processor 306 accesses to these buffers, the output processor 305 accesses to the output buffer 304 for non-RSVP. If a packet exists in the output buffers 304, the output processor 306 takes it out form the buffer 304.

Next, a reservation schedule function of VPN will be explained referring to Figs.5～6. As mentioned-above, while in the reservation of the network resources by using the original RSVP, the network resources are reserved only when the resources are necessary, in the present embodiment, by the following processes (I) ～(V), it is possible to designate a date or a time when the reserved bandwidth will be used. A step S28 in Fig.5 is continued to a step S29 in Fig.6.

(I) As steps S21 and S22 shown in Fig.5, when it occurs to reserve in advance a use of the resource reservation-type VPN, it is confirmed whether a setting of a section for an IP tunnel by RSVP is possible or not. If impossible, as steps S23 and S24, the reservation in advance is rejected.

(II) If the setting is possible, as steps S23 and S25 shown in Fig.5, it is confirmed whether an assurance of a bandwidth which will be

required at future date and time is possible or not. If impossible, as steps S26 and S24, the reservation in advance is rejected.

(III) If the assurance is possible, as steps S26 and S27, necessary information of the reservation (date, time, bandwidth to be reserved, IP address of sending side, IP address of receiving side, port number, protokol ID, etc.) are registered on a data-base for reservation in all routers on a section for an IP address.

(IV) On the designated date and term, as steps S28 shown in Fig.5 to S31 shown in Fig.6 and as following process ①~②, it is started to provide the reserved bandwidth.

① After a monitor during a predetermined period, as steps S28 and S24 shown in Fig.5, if no traffic exists from a host which reserved the bandwidth, the reservation in advance is rejected.

② As steps S29 and S30 shown in Fig.6, when a bandwidth is insufficient by a traffic which is not reserved in advance or not scheduled, one of following traffic controls (a) and (b) is carried out according to a kind of the non-reserved traffic.

(a) If a protokol of the non-reserved traffic is not RSVP, all the traffic is rejected.

(b) If a protokol of the non-reserved traffic is RSVP, a message for cancellation of its reservation is informed to its user, then the reservation is rejected.

(V) After the designated date and term, as steps S32 shown in Fig.6, it is finished to provide the reserved bandwidth.

According to embodiments of the present invention, it is possible to obtain a traffic characteristics which is not influenced by other traffics and more stabilized than conventional VPN, because of constructing an IP tunnel between routers connected with the INTERNET and reserving a

bandwidth of said IP tunnel by setting-up a reservation resource protokol (RSVP) on said IP tunnel. It is not necessary for each application to reserve a network resource because an assurance of a bandwidth by RSVP is carried out by an IP tunnel between routers, then it is not necessary for each host and/or sub-network to support RSVP. Setting and cancelling the assurance of the bandwidth are easy, because the bandwidth is assured by RSVP. Therefore, it is not necessary to change a parameter of each node by manual, then a human cost can be deleted. Further, it is possible to speedily and flexibly allocate the bandwidth according to a short-term demand. Furthermore, it is useful to transmit a large amount of data in short-term usage.

Further according to embodiments of the present invention, an algorism for the traffic control is very simplified, because, as a traffic control of said router on said IP tunnel, a frequency for sending packets, which are processed by an input processor and an output processor inside of said router, is allotted based on a ratio of the reserved bandwidth in each IP tunnel.

Furthermore, while in the reservation of the network resources by using the original RSVP, the network resources are reserved only when the resources are necessary, according to embodiments of the present invention, it is possible to reserve the assurance of the bandwidth on designated date and time in future, because each of routers on the IP tunnel has a function for scheduling the reservation and manages a time period at which VPN of a type of RSVP will be used.

WHAT IS CLAIMED IS:

1. A method for constructing a VPN having assured bandwidth comprising steps of:

a step of constructing an IP tunnel between routers connected with the INTERNET;

a step of reserving a bandwidth of said IP tunnel by setting-up a reservation resource protokol (RSVP) on said IP tunnel.

2. The method claimed in claim 1, wherein each of said routers on said IP tunnel has a function for scheduling a reservation and manages, based on the reservation schedule, a time period at which said reservation resource protokol is used.

3. The method claimed in claim 1 wherein, as a traffic control of said router on said IP tunnel, a frequency for sending packets, which are processed by an input processor and an output processor inside of said router, is allotted based on a ratio of the reserved bandwidth in each IP tunnel.

4. The method claimed in claim 2 wherein, as a traffic control of said router on said IP tunnel, a frequency for sending packets, which are processed by an input processor and an output processor inside of said router, is allotted based on a ratio of the reserved bandwidth in each IP tunnel.

5. A method for constructing a VPN having assured bandwidth substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

15

Application No: GB 9718373.5 **Examiner:** Keith Williams
Claims searched: 1-5 **Date of search:** 9 January 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PPA, PPS)

Int Cl (Ed.6): H04L 12/46, 12/56, 12/66

Other: Online WPI, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A,P	EP 0790751 A2 Lucent Technologies Inc. - see abstract	
A	Data Communications International, Vol.25, No.7, 21 May 96,USA, F Baker "Real-time services for router nets", pages 85-90, and INSPEC Abstract Number: B9608-6210R-015, C9608-5620-014	
A	IEICE Trans. On Communications, Vol.E78-B, No.8, Aug 95, Japan, H Esaki et al. "High speed datagram delivery over Internet using ATM technology", pages 1208-18, and INSPEC Abstract Number: B9512-6210L-032, C9512-5620W-013	
A	ConneXions, Vol.8, No.8, Aug 94, USA, B Braden et al.,"RSVP: a Resource reSerVation Protocol", pages 8-17, and INSPEC Abstract Number: B9504-6150M-011, C9504-5640-008	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.